Control System CCF Analysis

Revision 0

Non-Proprietary

November 2014

REVISION HISTORY

Revision	Date	Page	Description
0	November 2014	All	First Issue

ABSTRACT

This technical report (TeR) provides the results of the evaluation for postulated non-safety control system common-cause failures (CCFs) for APR1400.

TS

The pertinent features of the control systems, including the architecture of the distributed control system (DCS), credited in this evaluation are described in this technical report.

One key feature of the DCS that ensures the failure of a single non-safety control group does not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences (AOOs) in Chapter 15, is that major control functions, such as pressurizer level control and feedwater control, are distributed to separate control groups. Each control group consists of at least one separate controller and includes at least one control system.

The following Failure Types due to a shared signal failure and CSCCFs are evaluated to confirm that the DCD Chapter 15 analysis acceptance criteria are met.

- Failure Type 1 : multiple function failures due to a single failure of a shared signal
- Failure Type 2 : multiple failures of a single control group due to a CSCCF
- Failure Type 3 : multiple failures of more than one control group due to a CSCCF
- Failure Type 4 : multiple failures of Information Flat Panel Display (IFPD) control commands due to a CSCCF

For all Failure Types above, the failure effect on multiple control functions and multiple plant components is considered.

TS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF TABLES (Continued)

LIST OF FIGURES

ACRONYMS AND ABBREVIATIONS

AMI	automatic motion inhibit
AOO	anticipated operational occurrence
APR1400	Advanced Power Reactor 1400
AWP	automatic withdrawal prohibit
BAST	boric acid storage tank
BOP	balance of plant
CCF	common cause failure
CCS	component control system
CCW	component cooling water
CDP	condensate pump
CEA	control element assembly
CEAC	control element assembly calculator
Ch.	1) Chapter, 2) channel
CIAS	containment isolation actuation signal
CPCS	core protection calculator system
CPC	core protection calculator
CSCCF	control system common cause failure
CVCS	chemical and volume control system
CWP	1) CEA withdrawal prohibit, 2) circulating water pump
DCD	design control document
DCN-I	data communication network-information
DCS	distributed control system
DBE	design basis event
DNBR	departure from nucleate boiling ratio
DRCS	digital rod control system
DV	downcomer valve
ESCM	ESF-CCS soft control module
ESFAS	engineered safety features actuation system
ESF-CCS	engineered safety features – component control system
EV	economizer valve
FW	feedwater
FWCS	feedwater control system
HART	highway addressable remote transducer
HPPT	high pressurizer pressure trip

HSI	human-system interface
HTR	heater
HVAC	heating, ventilation, and air conditioning
I&C	instrumentation and control
I/O	input/output
IFPD	information flat panel display
IPS	information processing system
KHNP	Korea Hydro & Nuclear Power Co. Ltd.
LCO	limiting conditions for operation
LEL	lower electrical limit
LOCV	loss of condenser vacuum
LOF	loss of flow
LONF	loss of normal feedwater
LPD	local power density
MCR	main control room
MFIV	main feedwater isolation valve
MFWP	main feedwater pump
Mod.	modulation
MSIV	main steam isolation valve
MSIS	main steam isolation signal
MSSV	main steam safety valve
MTC	moderator temperature coefficient
NFO	not fully open
NIMS	NSSS integrity monitoring system
NPP	nuclear power plant
NPCS	NSSS process control system
NRC	Nuclear Regulatory Commission
NSSS	nuclear steam supply system
PA	postulated accident
Perm.	permissive
P&ID	piping and instrumentation diagram
PAMI	post accident monitoring instrumentation
P-CCS	process-component control system
PCS	power control system
PLCS	pressurizer level control system
POSRV	pilot operated safety and relief valve

PPCS	pressurizer pressure control system
PRV	process representative value
PZR	pressurizer
RCP	reactor coolant pump
RCS	reactor coolant system
RDT	reactor drain tank
RMS	radiation monitoring system
RPCS	reactor power cutback system
RRS	reactor regulating system
RSPT	reed switch position transmitter
RSR	remote shutdown room
SBCS	steam bypass control system
SFADL	specified acceptable fuel design limit
SIAS	safety injection actuation signal
Tavg	average temperature
TBV	turbine bypass valve
TBN	turbine
Tcold	cold leg temperature
TCS	turbine control system
Tref	reference temperature
VOPT	variable over power trip
UEL	upper electrical limit
UGS	upper group stop

Page intentionally blank

1. PURPOSE

The purpose of this technical report (TeR) is to determine the effects of the postulated common cause failures (CCFs) on the non-safety control system, describe the methodology for evaluating those function/component effects on the plant, and document the evaluation results for the Advanced Power Reactor 1400 (APR1400) design.

2. SCOPE

This TeR provides the evaluation methods and results of the evaluation for the postulated control system CCF (CSCCF).

TS

The expected failures due to a shared signal failure and CSCCF are divided into four parts as follows.

- Failure Type 1 : multiple function failures due to a single failure of a shared signal
- Failure Type 2 : multiple failures of a single control group due to CSCCF
- Failure Type 3 : multiple failures of more than one control group due to CSCCF
- Failure Type 4 : multiple failures of Information Flat Panel Display (IFPD) control commands due to CSCCF

TS

Failure Types 1 and 2 are evaluated to meet the AOO acceptance criteria of the DCD Chapter 15. Refer to Sections 5.1 and 5.2 for the evaluation method and the results.

Failure Types 3 and 4 are evaluated to meet the PA acceptance criteria of the DCD Chapter 15. Refer to Sections 5.3 and 5.4 for the evaluation method and the results.

3. APPLICABLE CODES AND REGULATIONS

The following subsections provide applicable codes and regulations.

3.1. 10 CFR 50.55a(h), “Protection and Safety Systems”

The 10 CFR 50.55a(h) endorses IEEE Std. 603.

3.2. IEEE Standard 603

The compliance with Clause 4.8 of IEEE Std. 603-1991 is described in this TeR.

The non-safety control system is designed to have the compliance with Clauses 4.8 and 5.6.3 of IEEE Std. 603-1991.

IEEE Std. 603-1991, Clause 5.6.3 states, in part, that the safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.

For the compliance with Clauses 4.8 and 5.6.3 of IEEE Std. 603-1991, the evaluation methods and results for the postulated CSCCF are described in this TeR.

4. CONTROL SYSTEM DESIGN FEATURES TO PREVENT CCF

This section describes design features of the non-safety control systems and safety systems that (1) prevent failures that could otherwise lead to a CCF, (2) reduce the adverse effect of CCFs or (3) allow coping with CCFs.

4.1. Credible Failure Boundary

TS

Most of the control systems are implemented by a DCS-based common platform that has been proven by operating experiences in the nuclear industry and other industries.

The DCS conducts the functions of operator interface, component level control, automatic process control, high-level group control, and data processing for normal operation. The DCS is designed with a redundant and fault-tolerant architecture for high reliability and to minimize and prevent the failure of a single component from causing a spurious plant trip.

Some instrumentation and control (I&C) systems are implemented by self-standing systems.

As the non-safety control systems are software-based systems that are susceptible to a software defect, the design features and evaluation are necessary to prevent CSCCF.

TS

4.2. Control System Overview

The non-safety control systems consist of the power control system (PCS) and the process-component control system (P-CCS).

The PCS includes the reactor regulating system (RRS), the digital rod control system (DRCS), and the reactor power cutback system (RPCS).

The P-CCS includes the NSSS process control system (NPCS) and balance of plant (BOP) control systems. The NPCS consists of the feedwater control system (FWCS), steam bypass control system (SBCS), pressurizer pressure control system (PPCS), pressurizer level control system (PLCS), and other miscellaneous nuclear steam supply system (NSSS) control functions.

The BOP control systems provide discrete and continuous control of normally used non-safety BOP processes including radwaste control system.

Major control systems of NSSS are PCS and NPCS which include RRS, RPCS, DRCS, PPCS, PLCS, SBCS, and FWCS. Refer to Figure 4.1-2.

4.3. Credible Failure Types of Control System CCF

Credible failures of the CSCCF are initiating events caused by the control system failure that can affect critical safety functions.

As each major control function is assigned to a separate control group which consists of at least one controller, the following 4 credible Failure Types are assumed as credible failures. Refer to Table 4.1-1.

- Failure Type 1 : multiple function failures due to a single failure of a shared signal
- Failure Type 2 : multiple failures of a single control group due to CSCCF
- Failure Type 3 : multiple failures of more than one control group due to CSCCF
- Failure Type 4 : multiple failures of IFPD control commands due to CSCCF

Table 4.1-1 Credible Failure Types

Failure Type	Evaluation Criteria
Failure Type 1 : Multiple function failures due to a single failure of a shared signal	To be bounded by DCD Chapter 15 AOO acceptance criteria
Failure Type 2 : Multiple failures of a single control group due to CSCCF	
Failure Type 3 : Multiple failures of more than one control group due to CSCCF	To be bounded by DCD Chapter 15 PA acceptance criteria
Failure Type 4 : Multiple failures of IFPD control commands due to CSCCF	

Refer to Figure 4.1-3 for the overview of the four Failure Types. The evaluation results of the four Failure Types are described in Section 5.

4.4. Control System Design Features

To reduce the likelihood of CSCCF, the control system is designed to have the following design features:

- Each control function in DCD Chapter 7.7 is assigned to separate control group that consists of at least one separate controller to limit the failure in the control group (segmentation)[1]. Refer to

Section 4.5.

- A redundant controller for increased availability
- Interlock/permissive functions by a separate control group or safety system to limit the failure effects (e.g., control element assembly (CEA) withdrawal interlock signals, turbine bypass valve (TBV) permissive signals)[2]
- Control signal validation to limit a single input failure of redundant channel inputs (i.e., large deviation of redundant inputs)
- Redundant analog input modules with auto signal selection algorithm to limit the failure effect of a single module (i.e., out of range)
- Hardwired signal interface of shared signals between the control groups within PCS and NPCS[3]
- Diagnostic and alarming functions
- Design features of the IFPD to defend against a design basis event (DBE) due to single random hardware failure (e.g., broadcast storm)[1]

[1] Control group segmentation and design features to protect broadcast storm are credited in the evaluation of Failure Types 1 and 2. For the design features of broadcast storm, refer to Section 4.4.5.

[2] Permissive functions of SBCS permissive control group are credited in the evaluation of Failure Types 1 and 2.

[3] Refer to Figure 4.1-3 and Table 5.1-1.

Each design feature listed above is described in the following sections.

4.4.1. Segmentation of Major Functions

Segmentation is a process that separates and groups components, including instrument and control functionality in a non-safety DCS controller.

Functional allocation is performed to minimize the effects of single failures in the nuclear power plant (NPP). Maintaining the dependent and independent relationships established by the plant functional design is achieved by allocating specific functions (e.g., monitoring, control) to specific processors and by allocating specific inputs and outputs to specific input/output (I/O) modules (e.g., boards, personality/base modules).

Segmentation is credited to limit the effects of a single failure within a controller to the functions controlled by that controller. However, even with segmentation, erroneous signals that may result from a single failure, and that propagate to other controllers, are evaluated in this analysis for their effect on the functions controlled by those other controllers.

Segmentation can also be credited to limit the effect of a software defect to a single controller, regardless of that defect existing in multiple controllers. This can be done by demonstrating that each controller has different inputs and application programs. Therefore, the same defect is unlikely to be triggered in multiple controllers concurrently.

Due to the continuous operation of most control systems, triggered failures are self-announcing because they cause component repositioning. Therefore, when the defect is announced, it can be corrected in all controllers, before it causes a CCF of multiple controllers.

The detailed requirements of segmentation are described in Section 4.5. Though the segmentation of control functions makes the concurrent failure of those multiple control functions highly unlikely, multiple concurrent failures of more than one control group due to a CCF is considered as a credible failure and is evaluated in Section 5.3 as a beyond design basis event.

4.4.2. Redundancy

The control system is provided with the following redundancies in the platform design:

- Digital processors
- Input/output modules
- Communication networks
- Power supply

Non-safety system cabinets include redundant power supplies with outputs auctioneered to power the digital processors, I/O modules, and other system peripherals. No loss of function occurs when either power supply is turned off or on, with the other supply being powered.

The non-safety system incorporates network communication configurations that have dual or redundant communication paths.

The non-safety system incorporates digital processors in configurations that have redundant processing. A failure that results in shutdown of the primary processor will automatically hand off system functionality to a backup processor. The non-safety system incorporates redundancy with selected inputs or outputs.

There are different approaches available to incorporate this redundancy. Depending on the approach taken, component and instrument segmentation are considered to that extent needed to preserve the desired fault tolerance for safety analysis.

A comprehensive set of diagnostics aids in fault detection, locating and repairing problems before they lead to more serious operational concerns. Failure of the primary controller would result in fail-over to the standby controller and an alarm. Failure of the standby controller would only result in an alarm as the primary controller is already controlling.

Redundancy enhances system availability due to many component failures. However, redundancy cannot prevent the adverse effects from a failure that results in erroneous or spurious signals.

Therefore, redundancy is not credited in the Failure Type 1, 2, 3 or 4 analyses.

4.4.3. Diagnostic and Alarming Functions

For all applications the non-safety DCS controller is provided in a redundant-pair configuration to provide fault tolerance. The non-safety DCS controller is fully redundant with a backup controller designed to operate in a masterless scheme. Each controller in the redundant pair executes the same application with the primary controlling the outputs while the secondary tracks the primary. Fail-over detection and switching control to the backup process controller is done automatically and smoothly.

The non-safety DCS controller utilizes multiple control areas to support multitasking and preemptive task scheduling. The controller has high-capacity control capability. The functions executed within one controller are typically limited only by the amount of memory or flash disk available, to execute simple or complex modulating and sequential control and by the throughput performance required for the application.

Diagnostic and alarming functions are not credited in the Failure Type 1, 2, 3 or 4 analyses.

4.4.4. Design Features of the Information Flat Panel Display

TS

TS

TS

4.4.5. Design Features to Prevent CCF Due to Broadcast Storms on the DCN-I Network

TS

4.4.6. Design Features to Cope with Broadcast Storms on the IFPD/ESCM Ethernet Networks

TS

TS

Figure 4.1-1 Credible Failure Boundary of Control System CCF

TS

Figure 4.1-2 Control System Overview

TS

Figure 4.1-3 Overview of 4 Credible Failure Types

TS

Figure 4.4-1 Data Communication between the IFPD and DCS Controller

4.5. Segmentation

A majority of the plant components do not possess a unique functional identity in that they are not individually important to the plant but are collectively important as a part of a subsystem or group. Looking at a system simplistically, the valves in a fluid flow path are of little importance without the pump that drives the fluid unless a major pressure difference exists. Conversely, the pump is of no value if the valves in a fluid flow path cannot be opened. This fundamental observation is the basis for the system configuration of the non-safety control system.

The grouping is performed on the non-safety control system design based on observing two levels of functional based grouping. This task is performed using the following methodology and definitions.

- Functional grouping - The first level of groupings establish a set of groupings that are consistent with functional boundaries of the physical systems, system definitions, and based on an overview of a grouping of systems and functions (e.g., primary systems, secondary systems, and support systems).

- Component groupings - The second level of groupings follow a very simplistic perspective to further group components defined by functional grouping consistent with functional plant processes.

The functional grouping and component grouping are not credited in the Failure Type 1, 2, 3 or 4 analyses.

After the functional grouping and component grouping, for CSCCF functional segmentation and component segmentation are applied to reduce the likelihood of potential credible failures, to mitigate the effects of the potential credible failures. The functional segmentation and component segmentation 1, 2 are described in Section 4.5.3, 4.5.4 and 4.5.5.

The functional segmentation and component segmentation are credited in Failure Type 1 and 2 analyses.

4.5.1. Functional Grouping

TS

TS

Figure 4.5-1 Critical Functions and Success Paths (Example)

4.5.1.1. Power Source Segregation

Plant components and the associated instrument loops are divided into the following power divisions:

Table 4.5-1 Segregation of Power Source

Power Division	Channel Designation
Non-Safety 'A'	AB (N1)
Non-Safety 'B'	BB (N2)

Components belonging to each division are grouped and assigned to controllers. Each division AB and BB have the required number of groups depending upon its ability to satisfy the design philosophy.

All controllers are redundant and are powered from two separate power supplies within the same electrical division. Therefore, a credible failure of a power source has no adverse effect on any control functions.

4.5.2. Component Grouping

TS

Figure 4.5-2 Independent Configuration (Example)

Figure 4.5-3 Serial Configuration (Example)

TS

Figure 4.5-4 Parallel Configuration (Example)

4.5.3. Functional Segmentation

TS

4.5.4. Component Segmentation 1

TS

Figure 4.5-5 Component Segmentation 1 for SBCS Turbine Bypass Control

TS

Figure 4.5-6 Component Segmentation 1 for High Pressure FW Heater

TS

TS

Figure 4.5-7 SBCS Main Functional Block Diagram

TS

Figure 4.5-8 SBCS Permissive Functional Block Diagram

TS

Figure 4.5-9 HP FW Heater Functional Block Diagram

4.5.5. Component Segmentation 2

TS

4.5.6. Control Group

Control groups are assigned in accordance with the functional segmentation and component segmentation 1 and 2.

Refer to Table 4.5-2 for the control group of non-safety control system.

Table 4.5-2 Control Group

TS

4.6. Redundant Controller for Availability Enhancement

The following equipment control logic circuits are designed as completely redundant control loop. The redundant control loop is provided with redundant controllers with two I/O modules. These control circuits perform their functions to be completely separated from each other. The redundant controllers and I/O modules access simultaneously the field data and if one controller or I/O module fail, the other controller or I/O module can perform automatically the functions of controller or data acquisition/signal initiation without bump.

- Control logic for RCPs
- Control logic for non-Class 1E 13.8 kV switchgear power circuit breakers
- Control logic for non-Class 1E 4.16 kV switchgear power circuit breakers

Any one failure is annunciated in the MCR and RSR.

4.7. Interlock/Permissive Functions by Separate Control Group or Safety system

TS

Table 4.7-1 Control Limit and Interlocks on Digital Rod Control System

Conditions of Interlocks	Functions	Signal Path
Upper electrical limit (UEL) and lower electrical limit (LEL) signals from reed switch position transmitter (RSPT).	Interlock: Blocks control rod withdrawal or insertion on automatic, manual group and manual individual DRCS control modes.	RSPT → DRCS (UEL, LEL)
Automatic withdrawal prohibit (AWP) signals from RRS and SBCS when Tavg is much higher than Tref, Tcold is high, or any opening demand of TBVs is generated in accordance with excessive energy in the NSSS.	Interlock: Blocks control rod withdrawal on automatic DRCS control mode.	RRS → DRCS (AWP) SBCS → DRCS (AWP)
Upper group stop (UGS) and lower group stop (LGS) function in the DRCS	Control Limit: Blocks control rod withdrawal or insertion on automatic and manual group DRCS control modes.	DRCS (UGS, LGS)
CEA withdrawal prohibit (CWP) signal from PPS.	Interlock: Blocks control rod withdrawal on automatic, manual group and manual individual DRCS control modes.	PPS → DRCS (CWP)

4.8. Control Signal Validation

Where there are at least three identical process parameter inputs including control and safety systems, a valid process representative value (PRV) calculated in the information processing system (IPS) are used to select a valid control signal, where necessary.

The control system takes action based on a sensor signal that is selected by a PRV that reflects a valid process representative value. PRV is used only as a reference value for a channel selection. One value is selected among Channel 1 and Channel 2 or average in accordance with control signal validation algorithm.

If the deviation between the input channels exceeds an acceptable level, the input channel that has less deviation from the PRV is used as the control signal.

Therefore, there are fewer challenges to plant safety due to control system errors, since failed sensors are detected and eliminated before they adversely impact control system performance.

IPS failure would affect the control function, only if there is an additional failure of an input channel. Refer to Subsection 7.7.1.1 of DCD.

TS

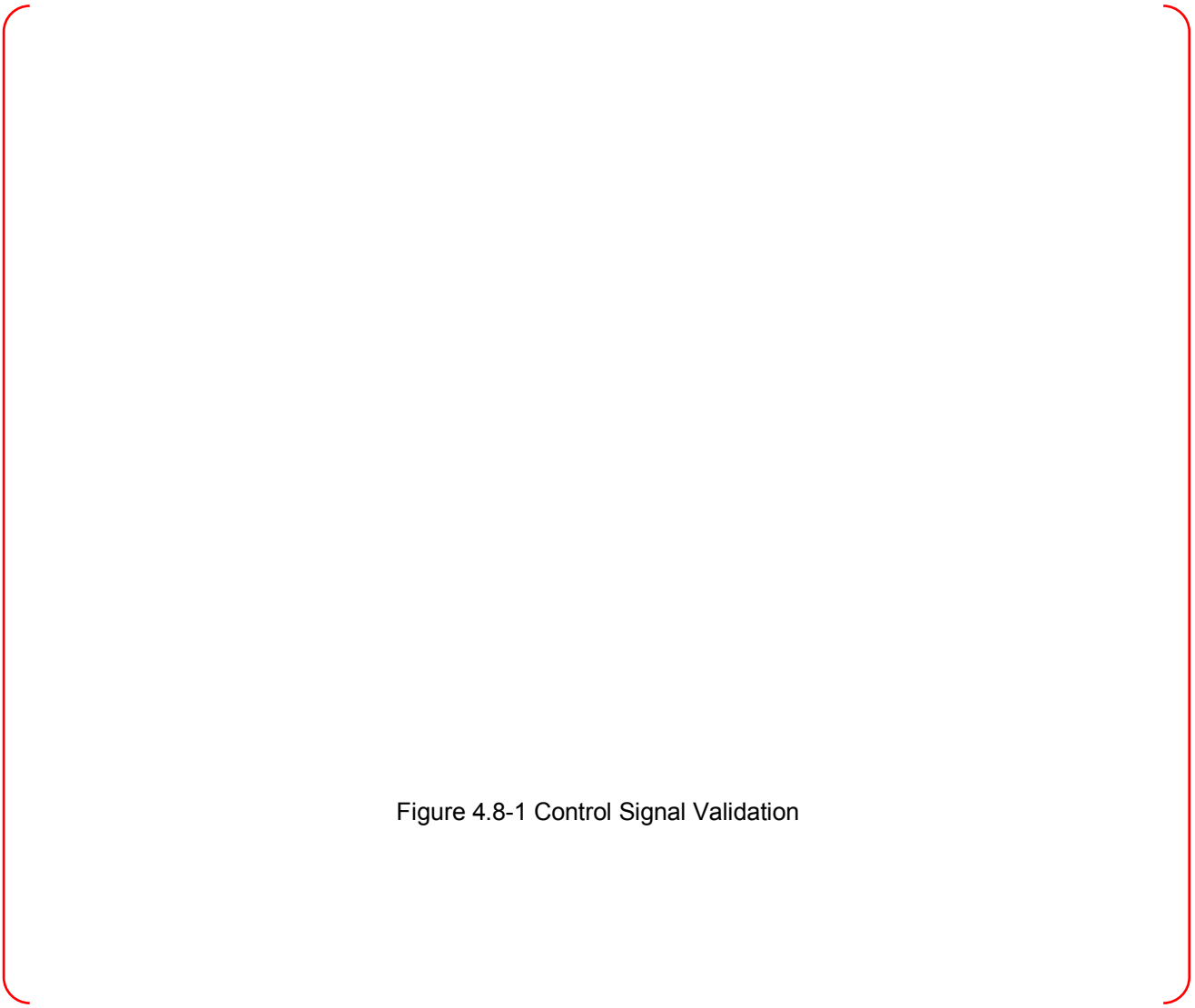

Figure 4.8-1 Control Signal Validation

4.9. Non-safety Control Signals Sent to ESF-CCS

TS

4.9.1. Evaluation of the Non-safety Control Signal for CVCS

TS

TS

Figure 4.9-1 Non-safety Control Signals Sent from P-CCS to ESF-CCS (Typical)

TS

Figure 4.9-2 ESF-CCS Control Logic against Non-Safety Signal Failure

4.9.2. Evaluation of the Non-safety Control Signal for Safety Smoke Damper Control

TS

Figure 4.9-3 Signal Flow from Non-safety Smoke Detector to Safety Smoke Damper

TS

Figure 4.9-4 Configuration of Control Room HVAC System

4.10. CCF Analysis of Embedded Devices in Field Equipment

TS

4.10.1. Evaluation for the CCF of Non-safety Field Instruments

4.10.2. Evaluation for the CCF of Non-safety Field Actuators

4.10.3. Evaluation for the Effect on Field Instruments due to Controller Failures

TS

4.10.4. Evaluation for the Effect on Field Actuators due to Controller Failures

TS

Table 4.9-1 Non-safety Control Signals sent from P-CCS to ESF-CCS

TS

Table 4.9-1 Non-safety Control Signals sent from P-CCS to ESF-CCS (cont'd)

TS

5. EVALUATION METHOD AND RESULTS

This section describes the evaluation methods and results for the postulated CSCCF of the control system. Depending on the Failure Types, limiting initiating events caused by CSCCF are selected and the qualitative evaluations are performed to verify that the results of initiating events are bounded by the same acceptance criteria of the design basis accidents presented in the DCD Chapter 15. Where necessary for some events, quantitative evaluations are performed to confirm that the analysis acceptance criteria are met.

The expected failures due to a shared signal failure and CSCCF are divided into four types as follows.

- Failure Type 1 : multiple function failures due to a single failure of a shared signal
- Failure Type 2 : multiple failures of a single control group due to CSCCF
- Failure Type 3 : multiple failures of more than one control group due to CSCCF
- Failure Type 4 : multiple failures of IFPD control commands due to CSCCF

TS

5.1. Failure Type 1: Multiple Failure due to a Single Failure of Shared Signal

TS

5.1.1. Assumptions Used in the Evaluation

TS

TS

TS

5.1.2. Initial Conditions

TS

5.1.3. Acceptance Criteria

TS

5.1.4. Evaluation Results

TS

TS

TS

TS

TS

TS

TS

TS

5.2. Failure Type 2: Multiple Failure due to Single Control group

TS

5.2.1. Selection of Initiating Events

5.2.2. Assumptions Used in the Evaluation

5.2.3. Acceptance Criteria

TS

5.2.4. Evaluation Results

TS

TS

TS

TS

TS

TS

TS

TS

TS

TS

5.2.5. Conclusion

5.3. Failure Type 3: Multiple Failures of more than One Control Group

TS

5.3.1. Selection of Initiating Events

5.3.2. Assumptions Used in the Evaluation

TS

5.3.3. Initial Conditions

5.3.4. Acceptance Criteria

5.3.5. Evaluation Results

TS

5.3.6. Conclusion

TS

5.4. Failure Type 4: Multiple Failures of IFPD Control Commands

Table 5.1-1 Shared Signals

TS

Table 5.1-1 Shared Signals (Continued)

TS

Table 5.1-2 Multiple Failure due to a Single Failure of Shared Signals (1 of 18)

TS

Table 5.1-3 Multiple Failure due to a Single Failure of Shared Signals (2 of 18)

TS

Table 5.1-4 Multiple Failure due to a Single Failure of Shared Signals (3 of 18)

TS

Table 5.1-5 Multiple Failure due to a Single Failure of Shared Signals (4 of 18)

TS

Table 5.1-6 Multiple Failure due to a Single Failure of Shared Signals (5 of 18)

TS

Table 5.1-7 Multiple Failure due to a Single Failure of Shared Signals (6 of 18)

TS

Table 5.1-8 Multiple Failure due to a Single Failure of Shared Signals (7 of 18)

TS

Table 5.1-9 Multiple Failure due to a Single Failure of Shared Signals (8 of 18)

TS

Table 5.1-10 Multiple Failure due to a Single Failure of Shared Signals (9 of 18)

TS

Table 5.1-11 Multiple Failure due to a Single Failure of Shared Signals (10 of 18)

TS

Table 5.1-12 Multiple Failure due to a Single Failure of Shared Signals (11 of 18)

TS

Table 5.1-13 Multiple Failure due to a Single Failure of Shared Signals (12 of 18)

TS

Table 5.1-14 Multiple Failure due to a Single Failure of Shared Signals (13 of 18)

TS

Table 5.1-15 Multiple Failure due to a Single Failure of Shared Signals (14 of 18)

TS

Table 5.1-16 Multiple Failure due to a Single Failure of Shared Signals (15 of 18)

TS

Table 5.1-17 Multiple Failure due to a Single Failure of Shared Signals (16 of 18)

TS

Table 5.1-18 Multiple Failure due to a Single Failure of Shared Signals (17 of 18)

TS

Table 5.1-19 Multiple Failure due to a Single Failure of Shared Signals (18 of 18)

TS

Table 5.2-1 Control Group Segmentation

TS

Table 5.2-1 Control Group Segmentation (Continued)

TS

Table 5.2-1 Control Group Segmentation (Continued)

TS

Table 5.2-2 Multiple Failures of Single Control group (SBCS Main)

TS

Table 5.2-3 Multiple Failures of Single Control group (SBCS Permissive)

TS

Table 5.2-4 Multiple Failures of Single Control group (FWCS1)

TS

Table 5.2-5 Multiple Failures of Single Control group (FWCS2)

TS

Table 5.2-6 Multiple Failures of Single Control group (PPCS)

TS

Table 5.2-7 Multiple Failures of Single Control group (PLCS)

TS

Table 5.2-8 Multiple Failures of Single Control group (CVCS)

TS

Table 5.2-9 Multiple Failures of Single Control group (RRS/RPCS) (Sh. 1 of 2) TS

Table 5.2-9 Multiple Failures of Single Control group (RRS/RPCS) (Sh. 2 of 2)

TS

Table 5.2-10 Multiple Failures of Single Control group (DRCS)

TS

Table 5.2-11 Multiple Failures of Single Control group (RCP)

TS

Table 5.2-12 Multiple Failures of Single Control group (HP FW Heater)

TS

Table 5.2-13 Multiple Failures of Single Control group (HP FW Heater Bypass Line)

TS

Table 5.2-14 Multiple Failures of Single Control group (FW Pump On/Off)

TS

Table 5.2-15 Multiple Failures of Single Control group (Non-1E AC Power to the Station Auxiliaries – 13.8kv)

TS

Table 5.2-16 Multiple Failures of Single Control group (Condenser Vacuum Control)

TS

Table 5.2-17 Multiple Failures of Single Control group (Turbine Control System)

TS

Table 5.2-18 Multiple Failures of Single Control group (Miscellaneous BOP control)

TS

Table 5.3-1 Assumptions for Event 1

TS

Table 5.3-2 Assumptions for Event 2

TS

Table 5.3-3 Initialization of RELAP5 for Nominal Initial Condition

TS

Table 5.3-4 Sequence of Major Events for Event 1

TS

Table 5.3-5 Sequence of Major Events for Event 2

TS

Table 5.4-1 Multiple Failures of IFPD control commands - Fuel Cladding Integrity

TS

Table 5.4-2 Multiple Failures of IFPD control commands - Primary System Integrity

TS

TS

Figure 5.3-1 Core Power (Event 1)

TS

Figure 5.3-2 Pressurizer Pressure (Event 1)

TS

Figure 5.3-3 Safety Injection Flow (Event 1)

TS

Figure 5.3-4 SG Pressure (Event 1)

TS

Figure 5.3-5 DNBR (Event 1)

TS

Figure 5.3-6 Core Power (Event 2)

TS

Figure 5.3-7 RCP Discharge Pressure – Short Term (Event 2)

TS

Figure 5.3-8 RCP Discharge Pressure – Long Term (Event 2)

TS

Figure 5.3-9 POSRV Flow (Event 2)

TS

Figure 5.3-10 SG Pressure (Event 2)

6. CONCLUSIONS

The following Failure Types caused by a shared signal failure and a CSCCF are evaluated to confirm that the event consequences of DCD Chapter 15 are still effective and the analysis acceptance criteria are met.

- Failure Type 1 : multiple function failures due to a single failure of a shared signal
- Failure Type 2 : multiple failures of a single control group due to a CSCCF
- Failure Type 3 : multiple failures of more than one control group due to a CSCCF
- Failure Type 4 : multiple failures of IFPD control commands due to a CSCCF

TS

The evaluation concludes that all multiple failures caused by a shared signal or a CSCCF do not cause plant conditions more severe than the acceptance criteria of the DCD Chapter 15 AOOs and PAs.

7. REFERENCES

1. NUREG-0800, USNRC Standard Review Plan, Revision 3, 15.0 Introduction - Transient and Accident Analyses, March 2007.

2. DI&C-ISG-04, “Highly Integrated Control Rooms – Communications Issues,” Rev. 1, 2009

3. IEEE Std. 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.”

8. DEFINITIONS

1. Acceptance Criteria — Practical and reasonable objective pass/fail tests that identify approved requirements. Criterion is qualitative or quantitative, and defines sufficiency, not optimality.

2. Penalty factor — A multiplicative number necessary to ensure that the CPCS calculate DNBR and LPD conservatively